

FILED

UNITED STATES DISTRICT COURT

JUN 21 2024

for the
Northern District of Oklahoma

Heidi D. Campbell, Clerk
U.S. DISTRICT COURT

In the Matter of the Search of)
A black Apple iPhone SE, S/N: JYRL4WF0QR and a black)
Lenovo ThinkPad computer, S/N: PF-2L53AR, Currently)
Stored at the Tulsa Police Department Computer)
Forensics Lab located at 3245 E 5th PL, Tulsa, Oklahoma)

Case No. 24-mj-430-SH**APPLICATION FOR A SEARCH WARRANT**

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment "A"

located in the Northern District of Oklahoma, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

*Code Section**Offense Description*

18 U.S.C. §§ 2252(a)(2) & (b)(1)

Distribution and receipt of Child Pornography

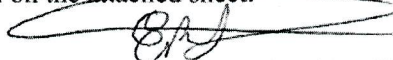
18 U.S.C. §§ 2252(a)(4)(B) & (b)(2)

Possession of or Access with Intent to View Child Pornography

The application is based on these facts:

See Affidavit of Eric Leverington, TFO, HSI, attached hereto.

- ☒ Continued on the attached sheet.
☐ Delayed notice of ____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


Applicant's signature

Eric Leverington, TFO, HSI

Printed name and title

Subscribed and sworn to by phone.

Date: 6/21/24

*Judge's signature*City and state: Tulsa, Oklahoma

SUSAN E. HUNTSMAN, U.S. Magistrate Judge

Printed name and title

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OKLAHOMA**

**In the Matter of the Search of
A black Apple iPhone SE, SIN:
JYRL4WF0QR and a black Lenovo
ThinkPad computer, S/N: PF-
2LS3AR, Currently Stored at the
Tulsa Police Department Computer
Forensics Lab located at 3245 E 5th
PL, Tulsa, Oklahoma**

Case No. _____

**Affidavit in Support of an Application
Under Rule 41 for a Warrant to Search and Seize**

I, Eric Leverington, being first duly sworn under oath, depose and state:

Introduction and Agent Background

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant authorizing the examination of property-black Apple iPhone SE, S/N: JYRL4WF0QR and black Lenovo ThinkPad computer S/N: PF-2L53AR which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Task Force Officer with Homeland Security Investigations (HSI) and have been since February 2019. I am currently assigned to the Tulsa Resident Agency of the Dallas, Texas field office. In addition to becoming a Task Force

Officer with Homeland Security Investigations (HSI), I have been employed as a Police Officer with the Tulsa, Oklahoma Police Department since July 6, 1998. I am currently assigned to the Tulsa Police Department Sexual Predator Digital Evidence Recovery Unit with a primary focus on child exploitation investigations. Since becoming a Task Force Officer with HSI, I have investigated violations of federal law, to include federal violations concerning child pornography and the sexual exploitation of children. I have gained experience through training in classes and work related to conducting these types of investigations. Further, as a Homeland Security Investigations Task Force Officer, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

3. As part of my duties as a HSI Task Force Officer, I investigate criminal violations relating to child pornography, including Advertising to Receive, Exchange, Produce, Display, Distribute, and Reproduce child pornography, and the production, transportation, distribution, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2551(d)(1), 2251A(b), and 2252. I have received training in the areas of child pornography and child exploitation and have observed and reviewed numerous examples of child pornography, as defined in 18 U.S.C. § 2256, in all forms of media. I have been involved in several child pornography investigations and am familiar with the tactics used by individuals who collect and distribute child pornographic material.

4. I am familiar with the facts and circumstances of this investigation. The facts set forth in this affidavit are based on my personal observations, knowledge obtained from other law enforcement officers, my review of documents related to this investigation, conversations with others who have personal knowledge of the events and circumstances described herein, and a review of open-source information including information available on the Internet. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact I or others have learned during the course of this investigation.

5. Based on my training, experience, and the facts set forth in this affidavit, there is probable cause to believe that evidence of violations of 18 U.S.C. §§ 2252(a)(2) & (b)(1) - Distribution and receipt of Child Pornography, and 18 U.S.C. §§ 2252(a)(4)(B) & (b)(2) - Possession of or Access with Intent to View Child Pornography will be located in the electronically stored information described in Attachment B and is recorded on the Devices described in Attachment A.

Jurisdiction

6. "[A] warrant may be issued to search for and seize any property that constitutes evidence of a criminal offense in violation of the laws of the United States." 18 U.S.C. § 3103a.

7. The requested search is related to the following violations of federal law:

a. Title 18, United States Code, Sections 2252(a)(2) and (b)(1) prohibit any person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any visual depiction that has been mailed, shipped, or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct; and

b. Title 18, United States Code, Sections 2252(a)(4)(B) and (b)(2) prohibit any person from knowingly possessing or accessing with the intent to view, or attempting or conspiring to possess or access with the intent to view, one or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

8. Venue is proper because the person or property described in this affidavit is located within the Northern District of Oklahoma. Fed. R. Crim. P. 41(b)(1).

Identification of the Device to be Examined

9. The property to be searched are a black Apple iPhone SE S/N: JYRL4WF0QR and black Lenovo ThinkPad computer S/N: PF-2L53AR, hereinafter the "Devices." The Devices are currently located at the Tulsa Police Department Computer Forensics Lab located at 3245 E 5th PL, Tulsa, Oklahoma.

10. The applied-for warrant would authorize the forensic examination of the Devices for the purpose of identifying electronically stored data particularly

described in Attachment B.

Definitions

11. The following definitions, inclusive of all definitions contained in 18 U.S.C. § 2256, apply to this affidavit and the attachments incorporated herein:

- a. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct;
- b. "Internet Protocol address" or "IP address" refers to a unique number used by a computer or electronic device to access the Internet. IP addresses can be dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses may also be static, which means the ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet;
- c. "Electronic Mail," commonly referred to as email (or e-mail), is a method of exchanging digital messages from an author to one or more recipients. Modern

email operates across the Internet or other computer networks. Email systems are based on a store-and-forward model; that is, email servers accept, forward, deliver, and store messages. Neither the users nor their computers are required to be online simultaneously; they need only connect briefly, typically to an email server, for as long a period of time as it takes to send or receive messages. One of the most common methods of obtaining an email account is through a free web-based email service provider such as, Outlook, Yahoo, or Gmail. Anyone with access to the Internet can generally obtain a free web-based email account;

d. A "hash value" or "hash ID" is a unique alpha-numeric identifier for a digital file. A hash value is generated by a mathematical algorithm, based on the file's content. A hash value is a file's "digital fingerprint" or "digital DNA." Two files having identical content will have the same hash value, even if the file names are different. On the other hand, any change to the data in a file, however slight, will change the file's hash value, even if the file name is unchanged. Thus, if two files have the same hash value, they are said to be identical, even if they have different file names;

e. "Cloud storage service" refers to a publicly accessible, online storage provider that can be used to store and share files in large volumes. Users of cloud storage services can share links and associated passwords to their stored files with others in order to grant access to their file collections. Such services allow individuals to easily access these files through a wide variety of electronic devices such as

desktop computers, laptops, mobile phones or tablets, from anywhere. Many services provide free access up to a certain size limit;

f. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state;

g. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years;

h. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form;

i. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person; and

j. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of

conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

Probable Cause

12. On or about August 17, 2023, the National Center for Missing and Exploited Children (NCMEC) received CyberTipline Report 171070639 from social media messaging company MediaLab/Kik. Kik reported that photographs consistent with child pornography were uploaded and shared by Kik user "mitchtwidd" on the Kik platform. On September 15, 2023, Detective Aubrey Williams with the Tulsa Police Department authored a State of Oklahoma search warrant for the Kik account associated with "mitchtwidd". On November 27, 2023, Detective Williams reviewed the returned materials and found at least three unique images she recognized as child pornography and four copies of the original photos. When I reviewed the three unique photos recovered from MediaLab/Kik, I observed one photo that showed a prepubescent female approximately three to five years old that was in a bathtub being forced to insert an adult male's erect penis into her mouth. I also observed a photo that showed a three- to five-month-old female that had an adult male's erect penis being forced into her vagina. Finally, I observed a female that appeared to be eight to ten years old being posed with her vagina being fully exposed.

13. The "mitchtwidd" account appeared to have extensive communication with another user called "meowmixxxxxxx". The two accounts exchanged more than 875 messages between April - June 2023. Kik user "mitchtwidd" sent user

"meowmixxxxxxx" four separate images Det. Williams recognized as child pornography. The metadata within the photos sent by "mitchtwidd" matched the child pornography photos located in the Kik return. On two separate occasions user "meowmixxxxxxx" sent user "mitchtwidd" non-pornographic images of a male child approximately 4-6 years old. The search warrant return also indicated that user "mitchtwidd" was registered to the email address mitchell.twidwell@gmail.com and most frequently used the IP address 172.126.102.30.

14. On September 19, 2023, Det. Williams authored a State of Oklahoma search warrant for the Google account associated with mitchell.twidwell@gmail.com. On September 21, 2023, Detective Williams received the search warrant return from Google. The account appears to have been active since at least August 5, 2010. It contained numerous photographs of Mitchell Dean TWIDWELL, including his Oklahoma and Nebraska state-issued driver's licenses and his TruGreen work photo.

15. On November 30, 2023, Det. Williams authored a State of Oklahoma search warrant for the AT&T account associated with the IP address 172.126.102.30. On December 15, 2023, she received a response from AT&T stating that the account is associated with subscriber Mitchell TWIDWELL who resides at 141 N College Ave, Tulsa, OK, and has a phone number of 402-805-0982. A search of the Tulsa County Assessor Office website on January 10, 2024,

showed Mitchell TWIDWELL as the owner of 141 N College Ave.

16. On March 20, 2024, Det. Williams authored a State of Oklahoma residential search warrant for 141 N College Ave, Tulsa, OK, 74110. The warrant was served on March 21, 2024, by members of the Tulsa Police Department Sexual Predator Digital Evidence Recovery Unit. Mitchell TWIDWELL was the only person located inside the residence and he agreed to a non-custodial interview in the street in front of his residence. Det. Williams and I interviewed Mitchell Dean TWIDWELL at that time. During the interview TWIDWELL made the following statements:

- He frequently used the username "mitchtwidd"
- His email address is mitchell.twidwell@gmail.com
- He used Kik to communicate with women he met on dating apps
- He moved the women from the dating apps to Kik for communication because this ensured privacy and eliminated a record of any text message history
- Investigators would find child pornography on his cell phone
- He had been viewing child pornography for approximately two years
- He received child pornography from dating apps - he communicated with moms who would send him child pornography
- He also received offers from moms who wanted to arrange meetups with their children in exchange for money
- He said he had most recently purchased child pornography 6 months

ago

- He said he purchased child pornography via PayPal
- When asked if he had ever given direction to mothers to perform sexual acts with their children, he said "in the spirit of just talking about general moms doing general things, in the spirit of conversation, like I was saying just kind of playing along and I like the mind game of the conversation."

17. Mitchell TWIDWELL's Apple iPhone 11 was located on his person, and it was seized so it could be examined at the Tulsa Police Department Sexual Predator Digital Recovery Lab. Det. Williams found at least ten photos and videos she identified as child pornography. Additionally, she found payment history between TWIDWELL's CashApp account and an account belonging to "meowmixxxxxxxx". When I viewed the photos and videos located on TWIDWELL's Apple iPhone I observed at least ten photos and videos of prepubescent females under 10 that were being forced to have oral and vaginal sex with adults.

18. On April 2, 2024, Det. Williams authored a State of Oklahoma search warrant for the Apple iCloud account associated with twidwell.mitchell@gmail.com. This was the iCloud account registered to the cell phone seized during the warrant service on March 21, 2024. On April 16, 2024, she reviewed the return and found ten files she recognized as child pornography. When I reviewed the files recovered from the Apple iCloud account, I observed five unique photos I recognized as child pornography and five copies of the originals. Two of the unique photos show

prepubescent females approximately eight to ten years old with their vaginas exposed with either adults or other children performing oral sex on them. Two additional photos show prepubescent females that are having adult male penis's being inserted into their vaginas. Finally, one photo shows a prepubescent female approximately 12 years old with her vagina exposed kissing another juvenile female.

19. On April 5, 2024, after serving a search warrant for TWIDWELL's Reddit account, username "u/jacksonreid_onlyfun", it was discovered that TWIDWELL was a member of numerous subreddits, including "r /Perv_Mom", "r /breedingfamilys", "r /BornToBeFucked", "r /Family_Nudity", and "r /MomSonIncest". Based on the return received from Reddit, TWIDWELL appeared to be very active on these message boards and left frequent comments including the following conversation found on the Incest Confessions subreddit:

Original Post	I want to raise a free use family but men aren't into that for some reason?
u/jacksonreid_onlyfun	This fucking one is! I'm trying to find a female to breed!
Original Post	So guys please read my previous post for reference as to what I'm talking about. My family has become a free use family over the past 7-8 months and it has been a lot of fun. Loads of stuff has

	<p>been happening, like at least once a week. I can't post that much so please let me know what to post next.</p> <ol style="list-style-type: none"> 1. My dad joining my sister and me in the shower 2. A family game night of strip picture which ended with the 4 of us together 3. My mom teaching me how to blow my dad 4. My sister, my mom, and me
u/jacksonreid_onlyfun	Need more girls only; moms daughters

A review of TWIDWELL's chat history on Reddit showed the following conversation between "u/jacksonreid_onlyfun" and a now-deleted account. The last message from TWIDWELL is him sending the user his Session ID number:

Creation Time	Updated Time	Username	Message
2023-12-20 04:05:01 UTC	2023-12-20 04:05:01 UTC	jacksonreid_onlyfun	Are they young? oY«:
2023-12-20 05:53:19 UTC	2023-12-20 05:53:19 UTC	[deleted]	Yes
2023-12-20 05:54:29 UTC	2023-12-20 05:54:29 UTC	jacksonreid_onlyfun	Please send them 5y-
2023-12-20 05:57:30 UTC	2023-12-20 05:57:30 UTC	[deleted]	My daughters are 15 and 13
2023-12-20 05:57:33 UTC	2023-12-20 05:57:33 UTC	[deleted]	Is that ok with you
2023-12-20 06:00:03 UTC	2023-12-20 06:00:03 UTC	jacksonreid_onlyfun	I wouldnaE™t want them if they werenaETMt
2023-12-20 06:01:03 UTC	2023-12-20 06:01:03 UTC	[deleted]	Sweet
2023-12-20 06:02:02 UTC	2023-12-20 06:02:02 UTC	2023-12-20 06:02:02 UTC	2023-12-20 06:02:02 UTC

20. On April 8, 2024, Tulsa Police Department Det. Raymond Ackermann returned to TWIDWELL's residence at 141 N College Ave to conduct surveillance. Det. Ackermann observed that TWIDWELL's VW Tiguan was no longer in the driveway, a no trespassing sign had been placed on the front door, and the rolling garage door appeared to be open slightly. Det. Williams located a Facebook profile for one of the women TWIDWELL had been messaging, Printace Broughton-Clark. Clark had posted photos of herself visiting TWIDWELL at his residence on March 19, 2024. On April 1, 2024, Clark began posting photos of TWIDWELL at her residence in Houston, Texas. TWIDWELL is frequently photographed with Clark's daughter who is approximately ten years old. On May 13, 2024, TWIDWELL was photographed at a pool party for Clark's birthday with Sophie and an unknown 2-4 year old child. TWIDWELL was photographed with Clark attending the Houston Astros Hello Kitty Night baseball game on May 14, 2024. There were also photos of TWIDWELL at a children's pool party.

21. On May 16, 2024, an arrest warrant was issued for Mitchell TWIDWELL from the Northern District of Oklahoma. The arrest warrant was entered into NCIC after it was discovered that TWIDWELL was possibly staying in Houston, Texas. Detective Aubrey Williams contacted the Texas Department of Public Safety and requested assistance locating TWIDWELL. On May 28, 2024, TWIDWELL was located by officers with the Texas Department of Public Safety (DPS) at 1317 El Camino Village Dr, Houston, Texas 77058. TWIDWELL was brought outside the home and arrested. Clark was approached and was asked if she would

consent to officers searching the home for TWIDWELL's devices, Clark allowed officers to preview her own cell phone on scene and then took officers to the living room where she identified a black Lenovo ThinkPad computer as TWIDWELL's. Clark then took officers to the bedroom where TWIDWELL had been staying and identified a black Apple iPhone as TWIDWELL's. TWIDWELL was transported and booked into the Harris County Jail. TWIDWELL's black Apple iPhone S/N: JYRL4WF0QR and black Lenovo ThinkPad computer S/N: PF-2L53AR were secured by Texas DPS officers to prevent the destruction of any possible evidence.

22. Clark and her ten-year-old daughter were interviewed; neither made disclosures of touching. However, during Clark's interview with law enforcement, she informed officers that TWIDWELL had told her that he had come down to Houston because he needed a fresh start because he was working through some sexual deviances and that he was addicted to pornography. Clark also informed officers that her daughter would sometimes sleep in the bedroom with her, while TWIDWELL would sleep on the floor of the bedroom.

23. On May 31, 2024, Homeland Security Investigations Agent Russell Hurst collected the devices from the Texas Department of Public Safety and shipped them to the Tulsa Police Department Computer Forensics lab, 3245 E 5th PL, Tulsa, Oklahoma, for forensic analysis.

24. On June 18, 2024 in the Northern District of Oklahoma an impaneled grand jury returned a true bill of indictment against TWIDWELL for the following offenses: COUNT ONE: 18 U.S.C. §§ 2252(a)(2) and 2252(b)(1) -

Receipt and Distribution of Child Pornography; and COUNT TWO: 18 U.S.C. §§ 2252(a)(4)(A) and 2252(b)(2) - Possession of Child Pornography in Indian Country.

25. The Devices are currently in storage at the Tulsa Police Department Computer Forensics lab, 3245 E 5th PL, Tulsa, Oklahoma. In my training and experience, I know that the Devices have been stored in a manner in which their contents are, to the extent material to this investigation, in substantially the same state as they were when the Devices first came into the possession of the Tulsa Police Department.

Technical Terms

26. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities

include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players

can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

- d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

- e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.
- f. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail,

and participating in Internet social networks.

- g. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static-that is, long-term- IP addresses, while other computers have dynamic-that is, frequently changed-IP addresses.
- h. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

27. Based on my training, experience, and research, and from consulting the manufacturer's advertisements and product technical specifications available online at <https://www.apple.com/iphone-se/specs/> and <https://www.lenovo.com/us/en/c/laptops/thinkpad/>, I know that the Devices have capabilities that allow them to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, computer, and FDA. In my

training and experience, examining data stored on devices of these type can uncover, among other things, evidence that reveals or suggests who possessed or used the Devices.

**Characteristics Common to Individuals
who Exhibit a Sexual Interest in Children and Individuals who Distribute,
Receive, Possess and/or Access with Intent to View Child Pornography**

28. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who distribute, receive, possess, and/or access with intent to view child pornography:

- a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity;
- b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts;

c. Such individuals almost always possess and maintain digital or electronic files of child pornographic material, that is, their pictures, videos, photographs, correspondence, mailing lists, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, videos, photographs, correspondence, and mailing lists for many years;

d. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis;

e. Based on my training and experience and speaking with other special agents, I know that such individuals have taken their electronic devices and storage media, which contain their collections of child pornography, with them when they have moved or changed residences;

f. Such individuals may also take it upon themselves to create their own child pornography or child erotica images, videos or other recordings,

or engage in contact sex offenses with children. These images, videos or other recordings may be taken or recorded covertly, such as with a hidden camera in a bathroom, or the individual may have child victims he or she is abusing in order to produce child pornographic or child erotica images, videos or other recordings. Studies have shown there is a high cooccurrence between those who traffic in child pornography and commit sex offenses with children. Such individuals may also attempt to persuade, induce, entice, or coerce child victims in person or via communication devices to self-produce and send them child pornography or to meet in person for sex acts. These images, videos or other recordings are often collected, traded, or shared;

g. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted"¹ it;

h. Such individuals also may correspond with and/or meet others to

¹ See *United States v. Carroll*, 750 F.3d 700, 706 (7th Cir. 2014) (concluding that 5-year delay was not too long because "staleness inquiry must be grounded in an understanding of both the behavior of child pornography collectors and of modern technology"); see also *United States v. Seiver*, 692 F.3d 774 (7th Cir. 2012) (Posner, J.) (collecting cases, e.g., *United States v. Allen*, 625 F.3d 830, 843 (5th Cir. 2010); *United States v. Richardson*, 607 F.3d 357, 370-71 (4th Cir. 2010); *United States v. Lewis*, 605 F.3d 395, 402 (6th Cir. 2010).)

share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography;

i. Based on my training and experience, I know that such individuals may use their financial information to buy and sell child pornography online and purchase software used to mask their online activity from law enforcement. For instance, individuals may purchase cryptocurrency such as Bitcoin to buy and sell child pornography online. The use of cryptocurrency provides a level of anonymity because it masks the user's identity when conducting online financial transactions and provides a means of laundering illicit proceeds. Financial information may provide a window into the identities of individuals seeking to buy or sell child pornography online by tying the illicit transactions back to the user. Financial information contained on an electronic device containing child pornography may also provide indicia of ownership. Further, based on my training and experience, I know that individuals involved in the trafficking of child pornography may use sophisticated software, such as router configuration software, virtual private networks, proxy servers,

cryptocurrency exchanges, or other anonymizing software, in conjunction with these illicit financial transactions to provide dual layers of anonymity and prevent law enforcement detection. Financial information may indicate which services were purchased to obscure an individual's identity;

j. Such individuals prefer not to be without their child pornography for any prolonged period of time. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

**Background on Child Pornography, Computers,
and the Internet**

29. I have had both training and experience in the investigation of computer- related crimes. Based on my training, experience, and knowledge, I know the following:

- a. Computers, smartphones² and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers and smartphones basically serve four functions in connection with child pornography: production, communication, distribution, and storage;

² Smartphones are a class of mobile phones and of multi-purpose mobile computing devices. They are distinguished from feature phones by their stronger hardware capabilities and extensive mobile operating systems, which facilitate wider software, internet (including web browsing over mobile broadband), and multimedia functionality (including music, video, cameras, and gaming), alongside core phone functions such as voice calls and text messaging.

b. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as "WiFi" or "Bluetooth." Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos;

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers and smartphones and tablets around the world. Child pornography can therefore be easily, inexpensively and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone;

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types - to include computer hard drives, external hard drives, CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices which are plugged into a port on the computer - can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that

photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual's person.

Smartphones and/or mobile phones are also almost always carried on an individual's person (or within their immediate dominion and control) and can additionally store media;

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion;

f. Individuals also use online resources to retrieve and store child pornography.

Some online services allow a user to set up an account with a remote computing service that may provide e-mail services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud" storage) from any computer or smartphone with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer, smartphone or external media in most cases; and

g. As is the case with most digital technology, communications by way of computer or smartphone can be saved or stored on the computer or smartphone used for these purposes. Storing this information can be intentional (i.e., by saving an e-mail as a file on the computer or smartphone, or saving the location of one's favorite websites in, for example, "bookmarked" files). Digital information can also be retained unintentionally

such as the traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer or smartphone user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

Specifics of Search and Seizure of Computer Systems

30. As described above and in Attachment B, this application seeks permission to search for records that might be found on the Device in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media, such as a cellular phone, smartphone, or tablet. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

31. I submit that there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for

years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data;

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space-that is, in space on the storage medium that is not currently being used by an active file-for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file;

c. Wholly apart from user-generated files, computer storage media-in particular, computers' internal hard drives-contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information;

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

32. As further described in Attachment B, this application seeks permission to

locate not only computer files that might serve as direct evidence of the crimes described on the warrant but also for forensic electronic evidence that establishes how the Device(s) were used, the purpose of the use, who used the Device(s), and when. There is probable cause to believe that this forensic electronic evidence will be on the Device(s) because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified;
- b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to

exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that logs the following: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation

information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement);

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when;

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators.

Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant;

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent;

f. I know that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

33. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that

computer data can be stored on a variety of computer systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, smartphones, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage. I also know that:

a. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software website, or operating system that is being searched;

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate

analysis of the equipment and storage devices from which the data will be extracted;

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of a premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

34. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media

that reasonably appear to contain some or all of the evidence described in the warrant and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

Electronic Storage and Forensic Analysis

35. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

36. I know that cellular telephones are often equipped with digital cameras and those phones possess the capability to transmit and/or store electronic images. I know that in many cases, cellular telephones maintain photographs of illegal activities, including advertising to receive and exchange child pornography, distribution and receipt of child pornography, and possession of or access with intent to view child pornography. These photos are sometimes stored in their cellular phones and often are transmitted or sent from one electronic media device to another. I also know that cellular phones may also contain notes regarding potential illegal acts that are recorded by the subject who possesses the electronics. Furthermore, I know that text messages and emails are often used by two or more

persons to communicate information regarding illegal activities, between principals and co-conspirators of those crimes.

37. I know that cellular telephones are utilized by the majority of individuals in the United States and have become a staple of communication between individuals using text messaging, visual and audible communications (telephone calls and FaceTime type communications) as well as applications like "Signal," "Reddit," and "Telegram," and "Kik." Additionally, individuals utilize their cellular devices to take pictures, keep notes, as a GPS (global positioning System) device, and even to conduct illicit or illegal activity. Communications on phones are kept for long periods and transferred from one phone to another when replaced. This is done through the use of Cloud storage and direct transfer conducted at the time of purchase or by the individual themselves. Individuals utilize this method as not to lose data that is stored on the phone such as contacts, photos, notes, and other important information to the individual. This data includes contacts used to conduct illegal activities to include advertising to receive and exchange child pornography, distribution and receipt of child pornography, and possession of or access with intent to view child pornography.

38. Cellular telephones are often used to facilitate offenses and allow criminals to maintain communication with each other before, during and after the commission of offenses. I am aware that cellular telephones have the capacity to store a vast amount of information, including but not limited

to: telephone numbers, voice messages, text messages, e-mail, photographs, videos, address books, records, phone call histories, contact and other information. This information may be contained on the cellular telephone.

39. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

- d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

38. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Devices to human inspection in order to determine whether it is evidence described by the warrant.

39. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in

the day or night.

40. *Methods of examination.* In conducting this examination, law enforcement personnel may use various methods to locate evidence and instrumentalities of the crimes under investigation, including but not limited to undertaking a cursory inspection of all information within the Devices. This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, particularly including keyword searches, I know that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with stored cellular device data, such as pictures and videos, do not store as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications associated with a cellular device, as it is impossible to know in advance all of the unique words or phrases investigative subjects will use in their communications. Consequently, often many communications in cellular device data that are relevant to an investigation do not contain any searched keywords.

Conclusion

41. Based on the information set forth in this affidavit, I submit there is probable cause to believe that 18 U.S.C. §§ 2252(a)(2) & (b)(1) - Distribution and receipt of Child Pornography, and 18 U.S.C. §§ 2252(a)(4)(B) & (b)(2)- Possession of or

Access with Intent to View Child Pornography, have been violated, and that evidence of these offenses, more fully described in Attachment B, are located on the Devices described in Attachment A. I respectfully request that this Court issue a search warrant for the property described in Attachment A, authorizing the seizure of the items described in Attachment B.

42. Based upon my training and experience, I have learned that criminals who utilize the Internet actively search for criminal affidavits and search warrants and disseminate them to other criminals as they deem appropriate, i.e., post them publicly online through forums. It is possible that additional suspects will be discovered during forensic analysis of electronic devices. Premature disclosure of the contents of this Affidavit and related documents may have a significant and negative impact on this continuing investigation and may jeopardize its effectiveness by alerting the potential target(s) to the existence and nature of the investigation, thereby giving them an opportunity to flee, or to destroy or tamper with evidence.

43. I request to be allowed to share this affidavit and the information obtained from this search with any government agency, to include state and local agencies investigating or aiding in the investigation of this case or related matters, and to disclose those materials as necessary to comply with discovery and disclosure obligations in any prosecutions from this matter.

Respectfully submitted,

A handwritten signature in black ink, appearing to be "E. Leverington", enclosed within a horizontal oval shape.

Task Force Officer Eric Leverington
Homeland Security Investigations

Subscribed and sworn to by phone on June 21, 2024

A handwritten signature in black ink, appearing to be "Susan E. Huntsman", written in a cursive style.

SUSAN E. HUNTSMAN
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to be Searched

The property to be searched is a black Apple iPhone SE, SIN: JYRL4WF0QR, and a black Lenovo ThinkPad computer, serial number PF-2L53AR, hereinafter the "Devices." The Devices are currently located at Tulsa Police Department Computer Forensics Lab located at 3245 E 5th PL, Tulsa, Oklahoma.

This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENTB

Particular Things to be Seized

All records on the Device(s) described in Attachment A that relate to violations of 18 U.S.C. §§ 2252(a)(2) & (b)(1)- Distribution and receipt of Child Pornography, and 18 U.S.C. §§ 2252(a)(4)(B) & (b)(2) - Possession of or Access with Intent to View Child Pornography including:

- A. Images/ videos/ gifs of child pornography or child erotica; files containing images/videos/gifs; and data of any type relating to the sexual exploitation of minors or a sexual interest in children, material related to the possession thereof, and data of any type related to any person employing, using, persuading, inducing, enticing, or coercing any minor to engage in any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting such visual depiction of such conduct, in any form wherever it may be stored or found, including, but not limited to:
 - i. Graphic Interchange formats and/or photographs, and other visual depictions of such Graphic Interchange formats (including, but not limited to, JPG, GIF, TIF, AVI, and MPEG) of child pornography; files relating to the distribution, receipt, or possession of child pornography, or information pertaining to an interest in child pornography;

ii. Files in any form containing the visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256 or relating to the sexual exploitation of minors; and

iii. Stories, text-based files, motion pictures, films, videos, and other recordings of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256 or relating to the sexual exploitation of minors.

B. Information, correspondence, records, documents or other materials pertaining to the possession, receipt or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, or pertaining to the sexual exploitation of minors or a sexual interest in children, that were transmitted or received using computer, cellular device, personal digital assistant, or some other facility or means of interstate or foreign commerce, common carrier, or the U.S. mail including, but not limited to:

i. Correspondence including, but not limited to, electronic mail, chat logs, and electronic messages, establishing possession, access to, or transmission through interstate or foreign commerce, including by United States mail or by computer, of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256 or relating to the sexual exploitation of minors or a sexual interest in children;

- iii. Any and all electronic and/or digital records and/or documents pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate commerce including by United States mail or by computer, any visual depiction of a minor engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256 or relating to the sexual exploitation of minors;
- iv. Any and all electronic and/or digital records and/or documents including any and all address books, names, and lists of names and addresses of minors visually depicted while engaging in sexually explicit conduct, defined in Title 18, United States Code, Section 2256; or relating to the sexual exploitation of minors;
- v. Any and all records of Internet usage including usernames and e-mail addresses and identities assumed for the purposes of communication on the Internet. These records may include billing and subscriber records, chat room logs, e-mail messages, and include electronic files in a computer and on other data storage mediums;
- vi. Any physical keys, encryption devices, dongles and similar physical items necessary to access computer equipment, storage devices or data;

vii. Any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data; and

viii. Files, records, programs, logs, electronic communications, scanning programs, financial records, hacking software, or router configuration software.

C. Records or other items which evidence ownership, use, or control of the Devices described in Attachment A.

D. Credit card information including but not limited to bills and payment records, including but not limited to records of internet access.

E. Any and all information, correspondence (including emails), records, documents and/or other materials related to contacts, in whatever form, with minors involving the production, possession and/or distribution of child pornography and the attempt or act of educating, enticing, coercing, or persuading a minor to engage in sexual acts.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage.

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.